Accountancy Business and the Public Interest
ISSN: 1745-7718

Volume: 41
Issue Number: 12

FIRMS USING ARTIFICIAL INTELLIGENCE TO CONDUCT FRAUD DETECTION TO COMPLEMENT GOVERNMENT INVESTIGATORS

HERBERT REMIDEZ

PhD, Director of the Business Analytics Program,
Associate Professor, Business Analytics Satish &
Yasmin Gupta College of Business, Rm 221, University of Dallas.

Abstract

This study examines the emerging risk posed by independent financial researchers using AI to detect fraud on behalf of the US government to Indian and other international firms operating in the United States of America. It analyzes data from court records, press releases, and media reports, and describes the tools, techniques, and outcomes of these independent financial research firms. Unlike other countries, the US has laws that allow private citizens from any country to receive substantial cash rewards for reporting fraud perpetrated by companies conducting business in the US, even when the fraud occurs outside the US. These laws do not require that persons submitting the reports have worked for the company or have insider knowledge. These independent researchers combine programs powered by artificial intelligence with public and private datasets to detect and report suspected fraud to the US government.

INTRODUCTION

Over the previous 30 years, approximately once every 10 years, the U.S. government has responded to shocks to man-made and natural disasters by authorizing emergency spending programs. Disaster-relief programs were created in response to the savings and loan crisis (1989), the 9/11 attacks (2001), the 2007-2008 financial crisis and the COVID-19 pandemic (2020-2021). Through six COVID-19 relief laws, the U.S. government allocated $4.6 trillion in emergency spending. While reliable estimates of the percentage of these funds that were improper payments are not available, conservative estimates are in the tens of billions of dollars. Fraud, waste and abuse in emergency funding programs is an ongoing problem because governments face a tradeoff between vetting all participants and delivering assistance promptly to those affected (Lewis, A., et al 2023).

The US Government Accountability Office (GAO) is an independent, non-partisan agency that examines how federal agencies spend taxpayers' dollars and is responsible for providing auditing, evaluation and investigative services for the United States Congress. Government program managers must develop and implement plans in accordance with the GAO-managed Standards for Internal Control in the Federal Government. The GAO publishes a fraud management framework, best practices to guide fraud risk management activities by federal agencies, audit guidelines and lessons-learned reports (U.S. Government Accountability Office, 2015). Combined, these resources assist agencies and disaster-relief program managers in their fraud prevention and detection efforts.

Legislation authorizing emergency spending programs rarely authorizes additional funding for fraud prevention or detection efforts. This lack of funding leaves government agencies without the resources to grow fraud-prevention staff and infrastructure in proportion to the funds they are charged with expeditiously disbursing. The under-resourced fraud management offices, coupled with the nature of disaster-relief programs, lead to an increase in the percentage of improper payments. Improper payments include overpayments, underpayments, payments attributed to fraud or abuse, and payments lacking sufficient documentation. Efforts by government agencies to rectify improper payments can extend for more than 10 years after the payments are made. Companies operating in the United States face severe penalties if they violate the terms of government disaster-relief funding. Unlike many other countries, the U.S. has laws that enable private citizens from any nation to receive significant cash rewards for reporting fraud committed by businesses in the U.S. These laws can apply even if the fraud occurred in other countries. Independent researchers are using AI to uncover suspicious activities by connecting documents (e.g., program regulations, Securities and Exchange Commission filings, company-published reports, websites) to public and commercial databases. While independent researchers play a role in uncovering suspicious activities, the government conducts investigations to determine whether the activities meet the criteria for taking civil and/or criminal action. The involvement of independent researchers adds an extra layer of reassurance for taxpayers about the fraud-detection system's robustness. The objective of this study is to extract insights by analyzing court documents, press releases, and media accounts related to investigations initiated against international firms following reports submitted by independent financial researchers.

Novelty and Contribution

The COVID-19 pandemic led governments around the world to introduce emergency disaster relief programs. The United States government allocated $4.6 trillion in emergency COVID-19 relief spending. Companies from around the world received these funds because their subsidiaries conducted business in the U.S., making the parent companies liable for improper payments. For the first time, the U.S. government worked with multiple independent researchers to recover funds that the government had not detected as fraudulent. The PPP and Bank Fraud Enforcement Harmonization Act of 2022 established a 10-year statute of limitation for bringing charges, which means companies around the globe face the prospect of investigations under this law through the year 2031 (Congress, 2022). This is the first paper to raise awareness of the risks international firms face from independent researchers and to analyze the results of investigations initiated by these firms.

LITERATURE REVIEW

Whistleblower Programs around the World

Most countries have whistleblower laws. In 2019, the EU passed the "Whistleblower Protection Directive." It requires member states to ensure that whistleblowers have effective internal and external channels to report breaches of EU rules, that reports be properly investigated and acted upon, and that whistleblowers are protected from retaliation. In India, the Whistle Blower Protection Act 2014 provides legal mechanisms for public servants to report illegal, unethical and illegitimate practices. Whistleblower laws vary along important dimensions: 1) who is eligible for whistleblower protections, 2) scope of protection for whistleblowers, 3) the types of reported activities protected, 4) variety of channels available, 5) confidentiality and anonymity protections, 6) anti-retaliation provisions, 7) institutions established to manage investigations, and 8) rewards available to incentivize whistleblowers.

Only a few countries have whistleblower reward laws. These include South Korea, Ghana, Canada, and the United States of America. Whistleblowers in South Korea can report violations related to fair competition, health, safety, consumer protection, the environment, and cartel activity. The program adjusted the incentive structure, leading to an increase in complaints. By 2024, the total rewards paid in relation to 178 cartel reports amounted to approximately USD $95 million (National Whistleblower Center, n.d.). Canadian citizens can receive rewards for reporting tax and securities fraud schemes. Between 2016 and 2022, the Ontario Securities Commission awarded eleven whistleblowers a total of USD $9 million (Ontario Securities

Commission, 2023). These dollar amounts pale in comparison to the rewards paid to whistleblowers in the USA.

United States Whistleblower Programs

The United States of America far exceeds other countries in the type of actions covered by whistleblower laws and the number of whistleblower programs. The oldest of these laws is the False Claims Act, also known as the Lincoln Law, because it was signed into law in 1863 by Abraham Lincoln, in response to contractors defrauding the Union Army during the Civil War. The False Claims Act addresses fraud against government-funded programs, not private firms. All federal and state whistleblower programs offer monetary incentives for reporting fraud. Rewards provided to whistleblowers reporting fraud through the False Claims Act program exceeded USD $400 million in 2024 for helping collect over USD $2.9 billion (U.S. Department of Justice, 2025).

Other whistleblower programs are administered by the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC). SEC whistleblowers have reported fraud related to stock price manipulation, initial public offerings, crypto assets, and corporate disclosures & financials. The SEC awarded over $255 million to 47 individuals in 2024. The CFTC collected over USD $162 million in fines and awarded $42 million to whistleblowers in 2024. Even corporate compliance offers are eligible. The IRS collected over USD $474.7 million through its whistleblower program and awarded over USD $123.5 million (Kohn, S., 2023).

None of these programs limits participation to US citizens or to individuals who have worked at the offending firm. The Department of Justice recently launched pilot programs for corporate fraud and antitrust violations not covered by existing programs. In addition, there are whistleblower programs for reporting motor vehicle safety violations, violations of wildlife protection laws, bank violations of anti-money laundering laws, and ship pollution. All states have whistleblower laws that mirror the federal False Claims Act. Some state laws go further than protecting taxpayer funds and extend to fraud against private insurers (Kohn, S., 2023).

Independent Researchers

The SEC whistleblower program and the False Claims Act have attracted small groups of serial whistleblowers who, through exploring public and private datasets, uncover fraud and report it to the appropriate government agency. An example of a private auditor who conducts investigations and uncovers fraud is Edward “Ted” Siedle. Mr. Siedle, a former SEC attorney, has received multiple whistleblower awards from the SEC and CFTC programs for reports related to bank conflicts of interest violations and to violations involving state and city government pension funds (Evans et al 2021). Integra Med Analytics is similar to Mr. Siedle in that it analyzes large amounts of public data to uncover fraud and report it to U.S. government whistleblower programs (Groden, S. & Carboni, L. 2019). Because of the broad nature of SEC and FCA regulations, both entities can lead to investigations affecting companies operating in countries around the world.

Activists Short Sellers

Not all stakeholders welcome the growth of independent researchers seeking a reward for uncovering fraud. Some argue that offering financial incentives for reporting fraud devalues the efforts of those who report fraud because it is the morally right thing to do. Others argue that fraud detection should be left to the government. This position is similar to the position that activists seeking to make money through short-selling stocks should be prohibited.

Activist short sellers conduct privately funded investigations to uncover misdeeds by publicly traded companies (Brendel, J. and Ryans, J. 2021). The misdeeds they uncover do not always meet the criteria for any of the available whistleblower programs, but are meaningful to shareholders. After conducting investigations and uncovering sufficient evidence, an activist short-selling firm shorts a stock. The process that activist short sellers follow of covertly investigating firms that they are not associated with is similar to the one that independent whistleblowers follow. Both groups aim to compile disparate data into evidence that supports a narrative of wrongdoing. The difference is that independent fraud investigators submit their report to the government and let the government conduct its investigation, whereas, after uncovering suspected wrongdoing, activist short-selling firms begin shorting the stock of the firm suspected of wrongdoing.

Companies “short” a stock by borrowing shares of stock in a company they believe will decrease in value when they eventually publicize the results of their investigation. The activist investor sells the borrowed shares at market price, with an agreement to return the same number of shares they borrowed by a given date. After selling the borrowed shares, the firm releases its report detailing the suspected wrongdoing. If other market participants view the allegations of wrongdoing in the report as credible, the targeted firm's share price decreases. If this happens, the activist investor can purchase the number of shares it borrowed at the now-lower price, return the borrowed shares, and profit from the difference between the price per share before and after their report.

The ability to short a stock is important because it incentivizes private citizens to uncover fraud that might have gone undetected by government regulators. Most researchers agree that the activists' short-selling firms serve an important role in markets. Companies subject to campaigns by activist short sellers tend to view them negatively and would like the government to prohibit short-selling. Private researchers reporting suspicious transactions to the US government through whistleblower programs are similar to activist short sellers in that they bear the cost of investigating suspicious behavior to profit by uncovering illicit behavior. Much as some companies disparage activist short sellers, some people argue that private researchers should not be allowed to profit by uncovering fraud.

Rewards

Although the US has many laws and programs that independent researchers can use to seek rewards for reporting fraud, the most commonly used is the False Claims Act, which was used in all the cases reviewed for this study. This law allows the government to seek penalties that exceed three times the amount of fraudulently obtained funds. When an independent researcher reports suspected fraud, the government investigates and determines whether the circumstances warrant action. If so, it offers the target company the opportunity to settle the matter and provides the independent researcher with a portion of the funds collected in the settlement. These settlements reward the independent researchers and can deter would-be fraudsters (Leder-Luis, 2023).

AI in Fraud Detection

Academics and industry personnel have leveraged information systems to uncover suspicious behavior for decades (Du Preez, A. et al, 2024). These systems have included rule-based systems, machine learning techniques (anomaly detectors, clustering, decision trees), and artificial intelligence systems that employ a combination of techniques and continuously update their models. Popular application areas include credit card fraud detection, financial statement analysis, and healthcare billing. AI systems can be grouped into generative systems or discriminative systems. Generative systems, such as ChatGPT and Gemini, generate text, images, and audio output based on distributions in their training datasets. Discriminative AI systems are used for classification or regression and return predictions based on conditional probabilities. For example, the probability that two records represent the same business.

Record-matching programs perform rudimentary matching and record deduplication by matching names with slight misspellings, accent marks, and abbreviations. They cannot recognize relationships within the data, like a group of people working for the same employer, or automatically update results to incorporate newly added information. Advanced features like these require artificial intelligence algorithms that "learn" from patterns as new data is made available. AI-powered entity resolution systems, such as the one provided by Senzing, Inc. (www.senzing.com), recognize common nicknames, misspellings, and variations in the same address. For example, the AI learning model equates Jim with James, Bill with William, and Mohammed with Mohammad. These systems also recognize and match address variations, such as 1 First St. and One 1St. Street. When new information is added, the AI-based software systems dynamically update. In simple terms, it "learns" and updates matches when new datasets are added to the data compendium or when the user changes a configuration setting. Some systems automatically detect when a record contains a unique identifier and match records containing the same unique identifier across a data warehouse.

Paycheck Protection Program

This study examines allegations of fraud by businesses that received Paycheck Protection Program loans. The US government enacted the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) in March 2020 to provide economic assistance to American workers, families, small businesses, and industries. The Paycheck Protection Program (PPP) was part of the CARES Act, designed to help small businesses continue paying workers and other qualifying expenses during the early part of the COVID-19 pandemic. Through private lenders, the program distributed 11.3 million loans totaling more than $786 billion. The government forgave the full amount of the loans if borrowers certified that they had used the funds in accordance with the program rules and lenders recommended forgiveness. More than 95% of the loans were forgiven (Lewis, A, et al, 2023). The government published loan-level data, regulations, and frequently asked questions that borrowers were required to adhere to.

Independent researchers matched loan recipient data with other public and private records to identify borrowers suspected of violating one of the program requirements and reported these to the government for further investigation. After receiving these reports, the government investigated without involving the independent investigators. In cases where the government determined there was sufficient evidence to suspect fraud that did not warrant criminal charges, the intervened and offered the businesses a settlement that involved repaying the original loan plus restitution. The results of these investigations and settlement announcements are public records.

Data Sources

AI-powered entity resolution systems require users to collect and prepare datasets for analysis. They excel when provided with data from multiple sources that contain disparate pieces of information about the entities. The US government makes payment transaction records available for free, except in limited circumstances related to national security. These transactions are commonly used as input for AI-powered entity resolution systems. The US Employee Benefits Security Administration publishes another popular dataset. This dataset contains company names, addresses and the number of employees participating in the health and retirement programs administered by private companies. Combined Paycheck Protection Program loan data, tax filings from the US Internal Revenue Service, and medical billing and provider information from the Centers for Medicare & Medicaid Services, the AI systems can search across millions of rows. Records from commercial data brokers are often incorporated into the dataset used by these AI systems.

MATERIALS AND METHODS

The main objective of this research is to examine the emerging risk posed by independent financial researchers using AI to detect fraud on behalf of the US government. These independent researchers have expertise not readily available to government investigators, leverage their ability to direct AI tools to analyze large datasets, and are incentivized by the potential reward paid by the US government.

This research examines documents collected through extensive searches of the US court system records, web scraping the US Department of Justice website, and keyword searches of news articles published between 2020 and 2025. The results were compiled into a database of fraud complaints submitted to the US government under the False Claims Act. Complaints filed by insiders working at the defendant firm or by those with first-hand knowledge of the fraud were excluded from this analysis.

RESULTS AND DISCUSSION

The database contained 18 independent researchers, either individuals or groups organized under a company, who filed two or more complaints with the US government alleging fraud against the US federal government. Most complaints alleged that a single corporation or group of related companies violated the program requirements. However, some complaints named more than 50 defendants. In these cases, the defendants were related only to the extent the complaint alleged each defendant violated the exact program requirement (e.g., receiving two loans when the program limited participants to one loan).

These 18 independent researchers filed 265 complaints in total, of which 67 led to settlements. Of the 67 settlements, the government published the full settlement amount paid by the defendant for 50 of these. The settlements paid by these 50 defendants totaled more than $234 million. Settlements involving subsidiaries of international firms included allegations that fell into one of three categories. The most common accusation was that the subsidiary did not count employees from the parent company as required when determining whether it met the program requirement that limited participants to firms with 300 or fewer employees. In those cases, the US subsidiary employed fewer than 300, but the parent organization employed more than 300 when the total included working outside the US. The second most frequent allegation connected to a settlement payout was that the parent company was based in a country prohibited from participating in the program (e.g., ties to the People’s Republic of China). In settlements where a foreign firm was a defendant, penalties ranged from 48% to 95% of the initial payment, with an average of 64%. These amounts do not include legal expenses incurred by the defendant firms.

In all cases reviewed for this study, the government provided the independent researchers with 10% of the funds received under the settlement. The average payment received by the independent researcher across all cases reviewed was $469,529. The False Claims Act requires anyone wanting to report fraud to file a formal complaint through the court system, which usually requires them to partner with an attorney. In most cases, the law firm representing the investigator works under a contingency agreement, meaning their compensation is taken from the settlement paid to the investigator (in these cases, a portion of the 10%). The funds received by the independent researcher after paying the attorney are treated as regular income for tax purposes, further reducing the net income.

CONCLUSION

International companies conducting business in the United States have to manage the emerging risk posed by independent financial researchers using AI to detect fraud on behalf of the US government. Because of a 2022 law, international and domestic firms face the prospect of being investigated in 2031 based on actions a worker at a US subsidiary took in 2021. This study describes the laws unique to the United States of America that power this phenomenon by providing rewards to independent researchers who uncover fraud against the government. AI supercharges fraud detection and increases the risk that international companies face of being investigated due to a complaint filed against them. Recent settlements driven by independent researchers who have harnessed these tools demonstrate the US government's willingness to embrace new fraud-detection methods. Because independent researchers bear all the costs of uncovering suspicious transactions, the US government is likely to continue accepting reports from them. These factors make it imperative that companies conducting business educate themselves about this emerging risk.

References

1) Bhushan, A., Mathew, B., Kannaiah, P. & Kotni, V. (2025). Artificial Intelligence in Auditing: Enhancing Accuracy and Efficiency in Public Interest Financial Reporting. Accountancy Business and the Public Interest, 41(02), 122-131.

2) Brendel, J. and Ryans, J. (2021), Responding to Activist Short Sellers: Allegations, Firm Responses, and Outcomes. Journal of Accounting Research, 59: 487-528. https://doi.org/10.1111/1475-679X.12356

3) Burns, J. (2020). Data mining for qui tam false claims act suits: Business opportunity for the technology age, or doomed goose chase? *Tulane Journal of Technology & Intellectual Property*, *22*(1), 2–29.

4) Du Preez, A., Bhattacharya, S., Beling, P. & Bowen, E. (2024). Fraud detection in healthcare claims using machine learning: A systematic review. *Artificial Intelligence in Medicine*, *160*, 103061. https://doi.org/10.1016/j.artmed.2024.103061

5) Evans, J.W., Sipe, S.R., Inman, M. and Gonzalez, C. (2021). Reforming Dodd-Frank from the Whistleblower's Vantage. Am Bus Law J, 58: 453-523. https://doi.org/10.1111/ablj.12191

6) Gardezi, H., Sharma, H., Sharma, D., Sangisetti, M., Dron, S. & Saxena. R. (2024). AI-Driven SHRM Strategies for Financial Risk Mitigation and Enhanced Returns. Accountancy Business and the Public Interest, 40(12), 116-122.

7) Groden, S. L., & Carboni, L. (2019). The Future of False Claims Act Litigation? Recent Cases Reinforce Compliance Risk of Outside Relators. *Journal of Health Care Compliance*, *21*(6).

8) Kom, L. (2020). Investigations of Fraud, Waste, Abuse, and Corruption in the Public Sector: A Survey of Organizational and Software-Based Aids and Obstructions. *CUNY Academic Works.* https://academicworks.cuny.edu/gc_etds/3624

9) Kurshan, E., Mehta, D. & Balch, T. (2024). AI versus AI in Financial Crimes & Detection: GenAI Crime Waves to Co-Evolutionary AI. In Proceedings of the 5th ACM International Conference on AI in Finance, 745-751.

10) Kohn, S. M. (2023). *Rules for whistleblowers: A handbook for doing what's right* (S. Watkins, Foreword). Lyons Press.

11) Leder-Luis, J. (2025). Can whistleblowers root out public expenditure fraud? Evidence from Medicare. *Review of Economics and Statistics*, *107*(5), 1169–1186. doi.org/10.1162/rest_a_01163

12) Lewis, A., Futch, K. & Steinhoff, J. (2023). Be better prepared for the next crisis: Through robust enterprise and fraud risk management. *The Journal of Government Financial Management, 71*(4), 24-30. Retrieved from https://www.proquest.com/scholarly-journals/be-better-prepared-next-crisis-through-robust/docview/3143009540/se-2

13) Ontario Securities Commission (2023). Update on the OSC whistleblower program 2016 to 2022. https://www.osc.ca/sites/default/files/2023-03/OSC-Whistleblower-Program-Update-Report-20230309.pdf

14) Congress. (2022, August 5). PPP and Bank Fraud Enforcement Harmonization Act of 2022 [Government]. U.S. Government Publishing Office. https://www.govinfo.gov/app/details/COMPS-16988

15) Shekhar, S., & Jetson, K. (2024). Can machine learning target health care fraud? Evidence from Medicare hospitalizations [Working paper]. Boston University. https://shubhranshu-shekhar.github.io/assets/pdf/22-job-market-paper.pdf

16) U.S. Government Accountability Office. (2015). *A framework for managing fraud risks in federal programs* (GAO-15-593SP). https://www.gao.gov/products/gao-15-593sp.

17) U.S. Government Accountability Office. (2025). *COVID-19 relief: Improved controls needed for referring likely fraud in SBA's pandemic loan programs* (GAO-25-107267). https://www.gao.gov/products/gao-25-107267.

18) U.S. Department of Justice, Office of Public Affairs. (2025). *National health care fraud takedown results in 324 defendants charged in connection with over $14.6 billion in alleged fraud* [Press release]. https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-324-defendants-charged-connection-over-146.

19) U.S. Department of Justice, Office of Public Affairs. (2025). *False Claims Act settlements and judgments exceed $2.9B in fiscal year 2024*. https://www.justice.gov/archives/opa/pr/false-claims-act-settlements-and-judgments-exceed-29b-fiscal-year-2024

20) U.S. Department of Justice, Criminal Division. (n.d.). *Criminal Division Corporate Whistleblower Awards Pilot Program*. Retrieved November 17, 2025, from https://www.justice.gov/criminal/criminal-division-corporate-whistleblower-awards-pilot-program

21) U.S. Securities and Exchange Commission. (n.d.). *Whistleblower Program*. Retrieved November 17, 2025, from https://www.sec.gov/enforcement-litigation/whistleblower-program

22) Xu, J. J., Chen, D., Chau, M., Li, L., & Zheng, H. (2022). Peer-to-peer loan fraud detection: Constructing features from transaction data. *MIS Quarterly, 46*(3), 1777-1792.